CS 444/544 Intro to Cybersecurity, Spring 2018

Instructor: Jed Crandall, crandall@cs.unm.edu

PGP info is on my website: https://www.cs.unm.edu/~crandall

Never hesitate to email me directly about anything. If you're emailing me something about a group assignment, always cc the members of your group unless there's some reason for privacy.

Office and office hours: Farris Engineering Center 3060 (I'm pretty sure that's the right number, just look for the "Big Brother is Watching You" poster on the third floor). My office hours for spring 2018 will be 2:00pm to 4:00pm on Mondays and Tuesdays.

Class meeting time and place: MWF from 1pm to 1:50pm, in CEC B146 (the lab in the basement of the Centennial Engineering Center). Attendance will not be recorded and will not be explicitly part of your grade, but I strongly encourage you to attend class regularly because we're going to move at a fast pace. That said, if you think you have the flu please do not come to class. I'll be happy to help you catch up on anything you miss and give extensions as necessary if you stay home because you don't want to infect other people with the flu.

Prerequisites: None formally, having taken CS 341 (Computer Organization and Design) or an equivalent class from your undergraduate institution before taking this class is generally recommended, and I'll generally assume that students have a 400-level understanding of systems, theory and algorithms, and programming skills. When I discuss systems issues such as context switches or system calls I will assume that all students understand these things as they would coming out of CS 341 and entering CS 481. We will review these topics briefly at the beginning of the semester and as they come up, so it's possible to do well in this class without having taken 341, but you must be able to program well (in any imperative language like C, Java, Python, or whatever) to do well in the class.

TA: We do NOT have a TA, if that changes I'll send out an update.

Mailing lists: There are two mailing lists, one required and one optional. See the course website for details.

Course website: http://www.cs.unm.edu/~crandall/secprivspring18/

I'll post lots of important stuff here, like the lab assignments, links to the mailing lists, *etc.*

Required text: NONE. There are three recommended texts that I'll draw material from: *Computer Security: Art and Science* by Matt Bishop, *Gray Hat Hacking: The Ethical Hacker's Handbook 4th Edition* by Regalado *et al.*, and *Cryptography Engineering: Design Principles and Practical Application* by Ferguson *et al.* A couple of other good books you should check out are *Silence on the Wire* by Michal Zalewski and *Cryptovirology* by Young and Yung. We'll use a lot of online resources such as Wikipedia, academic papers, and the RFCs. "The only laws on the Internet are assembly and RFCs" (see Phrack 65), so expect to do some digging for dirty little details.

Grading: The final grade will be calculated as: 100% labs. There will be no exams, and homeworks will not be graded. The overall grade will be out of 100, weighted as described above. For letter grade purposes, below 60 is an F, 60 and up is a D, 65 and up is a C-, 70 and up is a C, 75 and up is a C+, 80 and up is a B-, 82 and up is a B, 85 and up is a B+, 87 and up is an A-, and 90 and up is an A. I only

give A+'s in extreme circumstances.

Grades of “Incomplete” or “Withdrawal”, changes in grade mode, or any other special accommodations will only be considered in cases where circumstances arose that were outside the control of the student (such as a death in the family, medical issues, etc.). Losing a scholarship or visa status because of a low grade is a very serious issue, but it's up to you to do well in the classes you register for to make sure that doesn't happen, not up to the instructors of the classes you take.

Note: The grading standards on one or more labs will be different for undergraduates (CS 444) and graduates (CS 544).

Labs: There will be 4 labs, all weighted equally (*i.e.*, each is exactly 25% of your final grade). How each lab gets graded will be written on the lab assignment. For some labs, there will be a flag that each student must attain and the grade will be all or nothing based on that, and whatever code or writeup you turn in will simply be backup in case I suspect you didn't do your own work for the assignment. For other labs there may be group or individual presentations, a short writeup, or some other tangible product that you’ll turn in. *Tentatively*, the four labs are expected to be:

1. Something involving basic network security and privacy, that incorporates (at least) Wireshark, nmap, and Tor.
2. A lab where you carry out a chosen ciphertext attack to recover a message. We’ll be attacking AES over RSA with modern key lengths, not some kind of toy crypto.
3. A lab where we play Werewolves, which is a Linux game where the motto is, “if you’re not cheating you’re not trying.”
4. A lab involving file carving and digital forensics on a cell phone.

Programming is necessary---C or Python are recommended. You may use other scripting languages (*e.g.*, Ruby) or any language you like, but keep in mind that the TA (if one materializes) and I won't be able to help you as well in languages we don't know as we can in languages we do. In general, for any language we can give you general advice and take a quick look at your code, but in a 400- or 500-level CS class don't expect us to debug your code for you or do a lot of hand-holding to get you started. If you’re not familiar with concepts like how to use network sockets, how to apply bitmasks to data, how to cast data into different types and deal with raw data, or other things that you would learn in classes like CS 241 or CS 351, then you should come talk to me before attempting the course. It is a 400/500-level computer science course, so being a strong programmer is a prerequisite.

<u>Be sure to start early on the lab assignments and get the help you need to get them done.</u>

Late assignments will only be accepted in special circumstances (medical, *etc.*).

Homeworks: There will be about eight to ten relatively light (compared to labs) homework assignments throughout the semester. They will typically entail carrying out a basic task and then either writing a very short email or giving a 1-minute presentation in class.

UNM statement of compliance with ADA: “Qualified students with disabilities needing appropriate academic adjustments should contact the professor as soon as possible to ensure your needs are met in a timely manner. Students must inform the professor of the disability early in the class so appropriate accommodations can be met. Handouts are available in alternative accessible formats upon request.”

Statement about Title IX borrowed from Patrick Bridges: “No form of discrimination, sexual harassment, or sexual misconduct will be tolerated in this class or at UNM in general. I strongly encourage you to report any problems you have in this regard to the appropriate person at UNM. As described below, I must report any such incidents of which I become aware to the university. UNM

also has confidential counselors available through UNM Student Health and Counseling (SHAC), UNM Counseling and Referral Services (CARS), and UNM LoboRespect. UNM faculty, Teaching Assistants, and Graduate Assistants are considered “responsible employees” by the Department of Education (see pg 15 at http://www2.ed.gov/about/offices/list/ocr/docs/qa-201404-title-ix.pdf).

This designation requires that any report of gender discrimination which includes sexual harassment, sexual misconduct, and sexual violence made to a faculty member, TA, or GA must be reported to the Title IX Coordinator at the Office of Equal Opportunity (oeo.unm.edu).

More information on the UNM policy regarding sexual misconduct, including reporting, counseling, and legal options, is available online:

https://policy.unm.edu/university-policies/2000/2740.html”

Cheating and collaboration:

Every homework assignment and lab assignment, unless I specify otherwise, should be an individual effort where you do your own work and only discuss the assignment with your classmates at a high level.

Each lab will have a special section of the assignment writeup where I'll try to be as specific as possible about what is allowed or not allowed with respect to cheating and collaboration. In general, you are expected to do your own work, and for group work all group members are expected to contribute.

Even for labs where your grade does not depend on the writeup, if you copy and paste any material (English text, figures, etc.) from any source you must clearly delineate it and attribute it properly to its source. Representing the work and materials of others as your own will not be tolerated in this class. Anything that is a full sentence or more that was not written originally by you has to be in quotes or indented in italics with a reference to clearly indicate where the material came from. Even if it was an accident, any kind of plagiarism in this class will result in an F in the class and possibly further actions pursuant to UNM policy.

All university policies regarding these matters will be strictly enforced. Typically I'll give the cheating parties an F in the class and report the incident to the Dean of Students, but I may pursue further action in some cases.

Some lab assignments may be group efforts. I expect everybody to contribute, if some group members do all the work and others slack off, I consider that a fault of each and every member of the group individually. Doing all the work yourself is not an alternative to showing leadership.

You will often hear me say, “If you're not cheating, you're not trying.” You should always take this in the context of a given assignment, and still adhere to the policies above. What I mean by “If you're not cheating, you're not trying” is that if you're only doing the technical aspects of assignments in the prescribed manner, you may be missing easier (as well as more fun and educational) ways of completing the assignment. The above policies always apply, and you can always ask me if you're not sure if something will be appropriate or not.

My expectations of you as students

- **Be studious:** I'm fairly old-fashioned, I expect students to come to class, to come on time, to stay on task, to take the time to make sure they understand things well, *etc.* (But don’t come to class with the flu.)
- **Take responsibility for your own learning:** You're either registered for a 400-level class or for a graduate class, at a major research institution. If you find that coming to the regularly scheduled class time is a waste of time, then you're probably not taking responsibility for your

own learning. Don't expect me to spoon-feed you information that is already well-known, you don't want to pay ~$750 in tuition for me to tell you what's in a ~$90 textbook that you could read yourself if you wanted to. My job is to inspire you to *want to* learn everything there is to know about cybersecurity, even after the semester ends. A good philosophical approach for you to take in this class is to "teach the teacher."

- **Take responsibility for the learning of others:** You should look around the room and ask yourself two questions: "Do I trust these people to help create an environment where I'll be excited to learn about cybersecurity?" and "Should they trust me to do the same?" This can be as simple as, *e.g.*, doing a good job on your presentations so as no to waste people's time, but also asking questions, generating interesting discussions in class and on the mailing list, and being a leader in group assignments or just in general.
- **Do only excellent work:** Anything worth doing is worth doing well. Even if I'm only grading that you attained a flag for a lab and am not grading your accompanying writeup, you should do an excellent job on the writeup (including the English grammar) for your own self.
- **Show leadership and be a mentor:** Don't think that this class is only about cyberescurity. If someone in your group is not as strong as you are in, *e.g.*, networking or programming, help them learn and motivate them to get things done instead of doing everything yourself.

Material to be covered:

The class will conceptually be broken up into three areas:

- Cryptography and network security: Crypography content will include symmetric and asymmetric cryptography algorithms, ciphertext-only attacks, known plaintext attacks, chosen plaintext attacks, chosen ciphertext attacks, hash functions, message authentication, secure channels, side channels, random number generation, quantum computing, blockchains, and societal impact issues. You will not be qualified to design cryptographic protocols after taking this course, but you should be able to critique them in the most basic ways. Network security content will include ARP, TCP/IP, SSL/TLS, DNS, BGP, and various attacks against these different layers of the Internet, as well as insertion, evasion, and denial of service. After taking this course, you should be able to reason about how different attacks in different layers correspond with various attacker capabiliities and goals. We'll spend a lot of time considering the attack model of a state actor with control of the Internet infrastructure (*i.e.*, Internet censorship and surveillance). We'll discuss the moral aspects of cryptography research and try to apply these to network and computer security and privacy research in general.
- Systems security and vulnerabilities: Systems security concepts will include authentication, basic UNIX abstractions and access controls, covert channels, information flow, and a survey of policies and mechanisms (*e.g.*, Bell-LaPadula, Windows DACLs). After taking this course, you should be able to reason about what security and privacy protections a typical commodity operating system provides and does not provide. Vulnerability concepts will include secure design principles (*i.e.*, Saltzer and Schroeder), memory corruption (*e.g.*, buffer overflows), breaking out of jails, concurrency issues (*e.g.*, TOCTTOU), cross-site scripting, command injection, and weak DACLs. After taking this course, you should have formed your own general ideas about vulnerabilities and be able to apply that knowledge to future vulnerability types that don't exist yet. We'll discuss the unique threats that journalists and activists face compared to other users.

- Digital forensics and privacy: Digital forensics concepts will include file carving, steganography, physical attacks, malware, cryptovirology, and malware analysis. Malware includes not only viruses, worms, and the like but also “legitimate” programs that perform malicious functions such as built-in keyword censorship. After taking this course, you should be able to reason about what digital artifacts can be recovered with physical access to a machine or access to a malware sample. Privacy concepts will include onion routing (particularly Tor), web tracking and ad networks, research results from reverse engineering the privacy of programs, mobile security and privacy, and the frequency blocking/amplification properties of tin foil *vs.* aluminum foil (for hat making). After taking this course, you should understand and be able to explain the technical aspects of current debates (especially in the U.S.) about Internet privacy, particularly against mass government surveillance. We'll also discuss the societal impact issues surrounding debates about government surveillance.

In the beginning of the class, before we learn anything technical, we'll discuss ethical disclosure issues, University policies, legal issues, research ethics, and ethical hacking in general. Throughout the curriculum, where appropriate, I will point out new and emerging research areas.

Ethical scholarship and proper use of UNM resources

You're responsible for understanding the laws and UNM policies pertaining to everything we do in class. You are expected at all times to comply with all policies and laws, and to behave in an ethical and responsible manner. We'll cover this early in the semester, including University polices such as 2500 and 2520, privacy laws relevant to the use of tools such as Wireshark, ethical disclosure, *etc.*

Themes:

While there are not yet basic tenets that define the field of cybersecurity, there are some themes that we’ll touch upon repeatedly throughout the semester at different points. These include:

Information only has meaning in that it is subject to interpretation. This is a quote from *Computer Viruses: Theory and Experiments* by Fred Cohen. We’ll see, for example, that often during exploits the same bits of information are interpreted more than one way, and that evading network intrusion detection systems is simply a matter of exploiting differences in interpretation.

Information wants to be free. Thomas Jefferson said, “That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation.” We’ll see that it’s hard to do anything with information without leaking it, because everything you do tends to make copies of it.

Programming the weird machine. The nature of vulnerabilities is that a system as implemented presents a “weird machine” that the attacker can “program” to cause computations and side effects to occur that the system designers and implementers did not intend to be possible.

Cybersecurity is going through fundamental changes. Simplicity, separation, hierarchical thinking, and placing limits on what users can do have been the basic building blocks for cybersecurity theory

and practice for decades, but research trends are increasingly challenging this.

Homework assignment #1:

This assignment is due by email (to crandall@cs.unm.edu) before 11:59pm on Wednesday, January 24th, 2018.

First, you should join the class mailing list by following the link on the course web page. You should get a confirmation email. If you don't get a confirmation email within 24 hours of joining the mailing list send me an email and indicate with which email address you tried to join the mailing list.

Also make sure that you have a valid CS account so that you can log into the lab machines.

Then, you should send me an email with answers to the following questions, where your answers can range from a sentence to a paragraph (or more, if you like).

1. Did you join the secpriv mailing list and then confirm that you have a CS account to log into the lab machines? Did you also join the (optional) secpriv-chat mailing list?
2. Who are you? What is your major? Where are you from? What do you hope to learn in this class?
3. Do you think that learning about cybersecurity this semester will be empowering? If so, how so?
4. Do you understand all of the course policies related to cheating and collaboration and grading?
5. What **legal** (or at least past the statute of limitations or something like that) thing have you done in your life that is the most like hacking? (Doesn't necessarily need to involve computers).

If your answer to #4 is not yes or if you don't complete this assignment on time, I'll use the instructor drop feature of LoboWeb to drop you from the class. If you'd like to remain in the class but don't understand the policies, please ask me questions until you do understand.